Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claim 1: (Currently Amended) A method of authentication for Media Gateway, characterized in that the method comprises:

providing each of a Media Gateway and a Media Gateway Controller with an initial key to validate digital signatures;

~~each of~~ said Media Gateway and said Media Gateway Controller performing a registration between the Media Gateway and the Media Gateway Controller and generating a shared key having a specific lifetime during the registration of said Media Gateway with said Media Gateway Controller by validating signaling messages used in the registration using the initial key, wherein the signaling messages include a parameter for generating the shared key and an initial digital signature generated by the initial key~~when said Media Gateway registers with said Media Gateway Controller using said initial key~~;

for each call, said Media Gateway Controller and said Media Gateway authenticating a call message and a response message, each including a digital signature~~each message between the Media Gateway Controller and the Media Gateway~~ by using the shared key; and

said Media Gateway and said Media Gateway Controller updating said shared key when the lifetime of said shared key is expired.

Claim 2: (Currently Amended) The method according to claim 1, characterized in that the step of ~~each of~~ said Media Gateway and said Media Gateway Controller performing the registration and generating the shared key comprises:

the Media Gateway sending a register signaling message to said Media Gateway Controller, wherein said register signaling message includes a parameter for said Media Gateway Controller to generate the shared key and an initial digital signature generated by the Media Gateway using said initial key;

said Media Gateway Controller validating the initial digital signature generated by the Media Gateway using the initial key;

said Media Gateway Controller generating the shared key based on the parameter in said register signaling message and setting a lifetime of said shared key when the initial digital signature generated by said Media Gateway is validated;

said Media Gateway Controller sending a modification command to said Media Gateway, wherein said modification command includes a parameter for said Media Gateway to generate the shared key, a digital signature generated by said Media Gateway Controller using said initial key, and the lifetime of said shared key;

said Media Gateway validating the digital signature generated by said Media Gateway Controller by using said initial key; and

said Media Gateway generating the shared key based on the parameter in said modification command and setting the lifetime, when the digital signature generated by said Media Gateway Controller is validated.

Claim 3: (Currently Amended) The method according to claim 1, characterized in that the step of said Media Gateway Controller and said Media Gateway authenticating ~~each message~~the call message and the response message for each call comprises:

~~for each call,~~ said Media Gateway Controller attaching ~~a~~ the digital signature ~~generated by the Media Gateway Controller~~ using said shared key to ~~a~~ the call message, wherein the digital signature is generated by the Media Gateway Controller and wherein the call message is transmitted to said Media Gateway;

said Media Gateway validating said digital signature attached to said call message by using said shared key and returning a response message attached with a digital signature generated by the Media Gateway using said shared key to said Media Gateway Controller when said digital signature in said call message is validated; and

said Media Gateway Controller validating said digital signature attached to said response message by using said shared key and establishing a call connection when said digital signature attached to said response message is valid, otherwise denying the call.

Claim 4: (Previously Presented) The method according to claim 1, characterized in that the

step of said Media Gateway and said Media Gateway Controller updating said shared key comprises:

sending a notification command by said Media Gateway to said Media Gateway Controller to request said Media Gateway Controller to generate a new shared key, wherein said notification command includes a parameter for said Media Gateway Controller to generate the new shared key and a digital signature generated by said Media Gateway using the initial key;

said Media Gateway Controller validating the digital signature generated by said Media Gateway using said initial key;

said Media Gateway Controller generating the new shared key based on the parameter in said notification command and setting a lifetime of said new shared key, when the digital signature generated by said Media Gateway is validated;

said Media Gateway Controller sending a modification command to said Media Gateway, wherein said modification command includes a parameter for said Media Gateway to generate the new shared key, a digital signature generated by said Media Gateway Controller using said initial key and the lifetime of the new shared key;

said Media Gateway validating the digital signature generated by said Media Gateway Controller by using said initial key; and

said Media Gateway generating the new shared key based on the parameter in said modification command and setting the lifetime, when the digital signature generated by said Media Gateway Controller is validated.

Claim 5: (Original) The method according to claim 2, 3 or 4, characterized in that the algorithm used to generate a shared key by said Media Gateway Controller and said Media Gateway is different from the algorithm used to generate a digital signature by said Media Gateway Controller and said Media Gateway.

Claim 6: (Currently Amended) The method according to claim 2, 3 or 4, characterized in that a field~~/~~ or a packet of an expanded protocol is used to transmit said parameter for generating a shared key and said digital signature.

Claim 7: (Previously Presented) The method according to claim 1, characterized in that the lifetime of said shared key is time, or the number of times that said shared key can be used for authentication.